



- 1 -

In re Application of:
Goodman et al.

Serial No.: 09/931,629

Filed: August 16, 2001

Title: FLASH UPDATE USING A
TRUSTED PLATFORM MODULE

: Before the Examiner:
: Longbit Chai
:
: Group Art Unit: (not on tape)
:
: IBM Corp.
: Intellectual Property Law
: Dept. 972/B656
: P.O. Box 12195
: Research Triangle Park, NC 27709

DECLARATION UNDER 37 C.F.R. § 1.132

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

We, Steve Goodman, Randall F. Springfield, and James Hoff, are the inventors of the above-identified Application, and declare as follows:

CERTIFICATION UNDER 37 C.F.R. § 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on February 14, 2005.

Signature

Toni Stanley

(Printed name of person certifying)

RPS9-2001-0046

PATENT

1. In the invention as recited in the claims of the above-identified patent application, the trusted platform module ("TPM") is used to do the signature verification of the update to program, and also enables the flash memory to receive the update. This makes the process of putting a tampered update to the program in the flash memory much more difficult.

2. In an example where a TPM does not directly unlock the flash memory unit, there must be a software interface that is used to unlock the flash memory unit, even if signature verification is performed on the program update to be loaded. Once this software interface is understood, it would then be a fairly simple matter of programming to write an application that can unlock the flash memory unit and store anything that is desired within the memory unit.

3. In contrast, within the present invention as claimed, where the TPM directly unlocks the flash memory unit, storing a tampered image (or program update) within the flash memory unit is much more difficult. In addition to figuring out the software interface to unlock the flash memory unit, the person attempting to store a tampered image must also figure out how to fool the TPM into thinking the image and update are authentic. That would mean that such an attacker on the system would have to present both an authentic image and the individual users authentication information to the TPM before the TPM would unlock the flash memory unit. This is significantly harder to do than in the case without using the TPM.

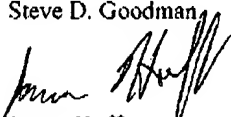
4. *Crawrock* teaches verification of the BIOS image after it has already been stored in the flash memory unit. The present invention verifies the BIOS image before allowing it to be stored in the flash memory unit and unlocking the memory unit.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this Declaration is directed.

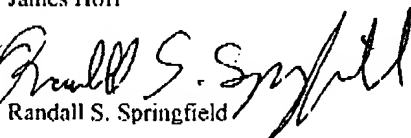
By:


Steve D. Goodman

By:


James Hoff

By:


Randall S. Springfield